PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-158660
(43)Date of publication of application : 31.05.2002

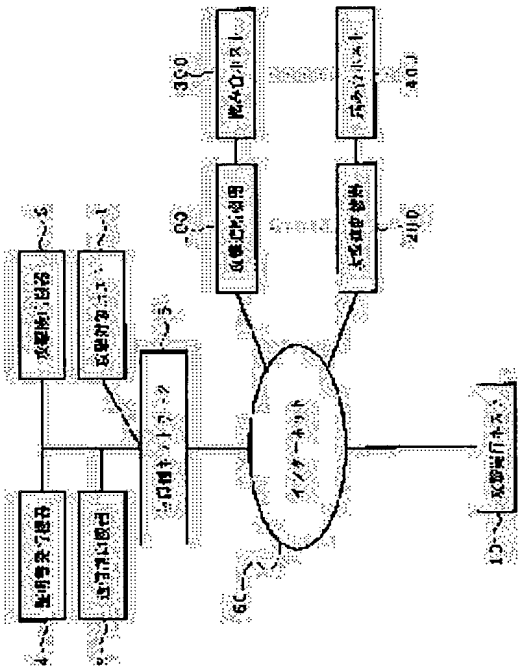
(51)Int.Cl. H04L 12/22
G06F 13/00
H04L 29/14

(21)Application number : 2000-355485
(22)Date of filing : 22.11.2000

(71)Applicant : NEC CORP
(72)Inventor : HARAGUCHI MINORU

(54) PROTECTION SYSTEM AGAINST UNAUTHORIZED ACCESS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a realistic protection means for coping with DDoS attacks, which impair the quality of service to be offered by performing large quantity of access to a specific host server.
SOLUTION: When footstool hosts 300 to 400 execute the DDoS attack as a large quantity of access to an attacking object host 1 by an instruction of an attack performance host 10, attack-detecting equipment 2 detects the attack by monitoring a state of a network 5 on the protecting side and communication control equipment 3 instruct communication control to attack shielding devices 100 to 200 by the instruction of a manager of the network on the protecting side 5, when the DDoS attack is detected by the attack detecting equipment 2. The footstool hosts 300 to 400 control communication, by receiving the instruction of communication control. In addition, certificate-issuing equipment 4 transmits information to assure the contents of the instruction of the communication control to the attack shielding devices 100 to 200.



LEGAL STATUS

[Date of request for examination] 22.10.2001
[Date of sending the examiner's decision of rejection] 06.04.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－158660
（P2002－158660A）
(43)公開日　平成14年５月31日(2002.5.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/22		Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｈ０４Ｌ　11/26		５Ｋ０３０
Ｈ０４Ｌ　29/14		13/00	３１１	５Ｋ０３５

審査請求　有　　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願2000－355485(P2000－355485)

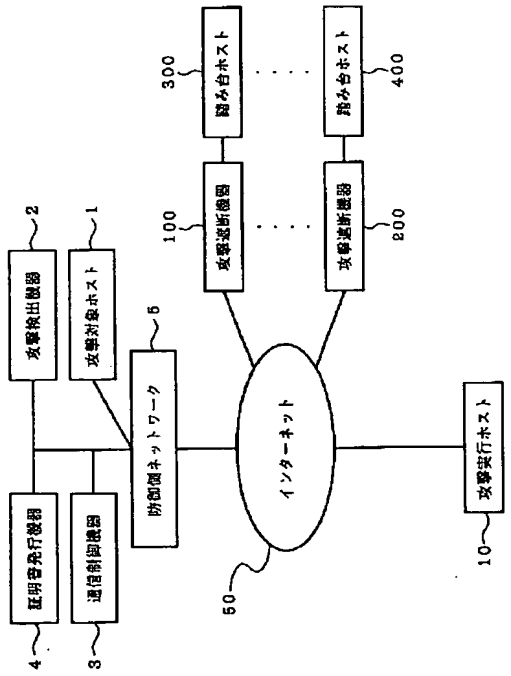
(22)出願日　平成12年11月22日(2000.11.22)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　原口　穣
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100086645
弁理士　岩佐　義幸

Ｆターム(参考)　5B089 GA04 GB02 JA35 JB16 JB22
KA17 KB13 MC02 MC08
5K030 GA15 HB11 HC01 HC13 LB02
LB03 LD19 MB09 MC08
5K035 CC03 DD01 EE08 MM04

(54)【発明の名称】　不正アクセス防御システム

(57)【要約】
【課題】　特定のホストサーバに大量のアクセスを行って提供するサービスの品質を損なうＤＤｏＳ攻撃に対応する現実的な防御手段を提供する。
【解決手段】　攻撃実行ホスト１０の指示により踏み台ホスト３００～４００が攻撃対象ホスト１に対して大量のアクセスであるＤＤｏＳ攻撃を実施すると、攻撃検出機器２は、防御側ネットワーク５の状況を監視してＤＤｏＳ攻撃を検出し、通信制御機器３は、攻撃検出器機２がＤＤｏＳ攻撃を検出した場合に、防御側ネットワーク５の管理者の指示により攻撃遮断機器１００～２００に通信制御の指示を出す。踏み台ホスト３００～４００は、通信制御の指示を受け取って通信を制御する。また、証明書発行機器４は、通信制御の指示の内容を保証する情報を攻撃遮断機器１００～２００に送信する。



【特許請求の範囲】
【請求項１】防御側ネットワークの状況を監視して攻撃対象ホストに対する不正アクセスを検出する攻撃検出機器と、
前記攻撃検出器機が不正アクセスを検出した場合に、前記防御側ネットワークの管理者による通信制御指示を出す通信制御機器と、
物理的に離れた前記不正アクセスを実施するホストに所属し、前記通信制御指示を受け取って通信を制御する攻撃遮断機器と、を備えることを特徴とする不正アクセス防御システム。
【請求項２】前記不正アクセスは、急激に増加するアクセスであることを特徴とする請求項１に記載の不正アクセス防御システム。
【請求項３】前記攻撃遮断機器の通信を制御する責任が前記防御側ネットワークの管理者にあることを保証する情報を前記攻撃遮断機器に送信する証明書発行機器をさらに備えることを特徴とする請求項１または２に記載の不正アクセス防御システム。
【請求項４】防御側ネットワークの状況を監視して攻撃対象ホストに対する不正アクセスを検出した場合に、防御側ネットワークの管理者の指示により、物理的に離れた前記不正アクセスを実施するホストに所属する攻撃遮断機器の通信を制御することを特徴とする不正アクセス防御方法。
【請求項５】前記不正アクセスは、急激に増加するアクセスであることを特徴とする請求項４に記載の不正アクセス防御方法。
【請求項６】前記攻撃遮断機器の通信を制御する責任が前記防御側ネットワークの管理者にあることを保証する情報を前記攻撃遮断機器に送信することを特徴とする請求項４または５に記載の不正アクセス防御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、特定のホストサーバへの不正なアクセスに対して防御を行う不正アクセス防御システムに関する。
【０００２】
【従来の技術】インターネットにおけるサービス妨害に、ターゲットとなるホストに多量のアクセスを行い負荷を増加させることによってターゲットとなるホストの提供するサービスの品質を損なう分散サービス拒否攻撃（ＤＤｏＳ攻撃：Ｄｉｓｔｒｉｂｕｔｅｄ　Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ攻撃）による妨害がある。
【０００３】ＤＤｏＳ攻撃の特徴として、攻撃を行う側から直接攻撃対象のネットワークまたはホストに対して攻撃を行うのではなく、攻撃を行うためのエージェントプログラムをインターネット上の多数のサーバに設定し、それに対して攻撃指示を与えることでターゲットのネットワークに対して攻撃を行うという間接的な方法であることと、個々のアクセスは正当なアクセスであっても、アクセス量がターゲットとなったネットワークまたはホストの限界を越えた非常に多量のアクセスであることが問題となるため、攻撃が始まって以降の対応が難しいこととがあげられる。
【０００４】ＤＤｏＳ攻撃の方式は、実行者のネットワーク環境の性能限界を越えたアクセスを実現するために実際に攻撃を行うホストを分散し、多数利用するために生み出された手法であるとも言える。
【０００５】従来、この種の「インターネットにおける分散サービス拒否攻撃に対するルータネットワークによる能動的な防御方法に関する発明」に相当する技術はなく、ＤＤｏＳ攻撃の踏み台に利用されないようにネットワークセキュリティを高めるか、特定パケットを一定量以上通過させないよう設定するかなど、何れも踏み台にされる側でセキュリティを高める方法のみが「２０００年１２月、情報処理振興事業協会発行、平成１１年度電子計算機利用技術の高度化調査―インターネット先進利用技術に関する調査研究」および「２０００年３月、日経オープンシステム、２０００年３月号、オープンレポート、１００頁」に発表されている。
【０００６】一旦、ＤＤｏＳ攻撃が開始されてからは、攻撃が終了するまで待つか、踏み台に利用されている多数ネットワークの管理者に対して個別にアクセスの遮断を依頼するかの方法しかない。
【０００７】
【発明が解決しようとする課題】しかしながら、上述した従来技術には、以下の問題点がある。
【０００８】第１に、現時点では攻撃を受ける側からの防御手段がないことである。ＤＤｏＳ攻撃への対応方法には、踏み台にされないようセキュリティを高める方法しか存在しないが、全てのネットワークがセキュリティを高め、かつそれを最新の状態に維持しない限り、踏み台にされうるネットワークはインターネット上に多数存在する。攻撃者は、手当たり次第に最新のセキュリティ対策を施されていないネットワークを探し、対策を施されたネットワークは単に無視すれば良い。
【０００９】第２に、攻撃が開始されてからの対応が事実上不可能ということである。攻撃が開始されたのを管理者が検知して以降は、攻撃を受けたネットワーク管理者から踏み台とされたホスト側に対して個別に対応を依頼する以外に対応方法がないが、数千台以上にのぼるホストの全管理者に対して依頼を行うのは事実上不可能である。
【００１０】本発明は、ＤＤｏＳ攻撃を受ける側からの責任において、ＤＤｏＳ攻撃が開始されて以降に本攻撃の影響を低減する方法を効率良く提供することを目的とする。
【００１１】
【課題を解決するための手段】本発明は、防御側ネット

ワークの状況を監視して攻撃対象ホストに対する不正アクセスを検出する攻撃検出機器と、前記攻撃検出器機が不正アクセスを検出した場合に、前記防御側ネットワークの管理者による通信制御指示を出す通信制御機器と、物理的に離れた前記不正アクセスを実施するホストに所属し、前記通信制御指示を受け取って通信を制御する攻撃遮断機器と、を備えることを特徴とする。

【００１２】また、前記攻撃遮断機器の通信を制御する責任が前記防御側ネットワークの管理者にあることを保証する情報を前記攻撃遮断機器に送信する証明書発行機器をさらに備えることを特徴とする。

【００１３】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１４】本発明は、インターネットにおけるＤＤｏＳ攻撃に対して、ネットワーク上で通信経路の制御を、ＤＤｏＳ攻撃の被害者側からの責任および操作によって、新たなＤＤｏＳ攻撃の発生に影響されることなく行う構成を提供するものである。

【００１５】図１は、本発明の不正アクセス防御システムの実施の形態を示す構成図である。図１に示す不正アクセス防御システムは、攻撃対象ホスト１、攻撃検出機器２、通信制御機器３、証明書発行機器４、防御側ネットワーク５、攻撃実行ホスト１０、インターネット５０、攻撃遮断機器１００～２００、踏み台ホスト３００～踏み台ホスト４００とにより構成される。

【００１６】攻撃対象ホスト１は、ワークステーション・サーバなどの情報処理装置である。攻撃対象ホスト１は、WWWサービスなどインターネット上にサービスを提供する機器として機能している。

【００１７】攻撃検出機器２は、ネットワーク負荷監視装置である。防御側ネットワーク５の管理者は、本装置によりネットワークの利用状況を監視し、ネットワーク負荷が急激に増加した場合に、ＤＤｏＳ攻撃が発生したケースを想定し、ネットワーク負荷が増加した要因を調査し、その負荷がＤＤｏＳ攻撃によるものかどうかを判断する。

【００１８】ＤＤｏＳ攻撃の発生によるものであると判断された場合、攻撃検出機器２は、通信制御機器３に対してＤＤｏＳ攻撃への対応指示を行う。

【００１９】通信制御機器３は、防御側ネットワーク５上に設置されたワークステーション・サーバなどの情報処理装置である。通信制御機器３上では、通信制御の指示を出すためのアプリケーションソフトウェアが動作しており、攻撃検出機器２からの指示に従い、さらに攻撃遮断機器１００～攻撃遮断機器２００に対して攻撃実行ホスト１０からの通信遮断指示を行うと同時に、証明書発行機器４に対して指示の妥当性の保証を依頼する。

【００２０】証明書発行機器４は、防御側ネットワーク５上に設置されたワークステーション・サーバなどの情報処理装置である。証明書発行機器４上では、通信制御機器３からの通信遮断指示が確かに防御側ネットワーク５の管理者から発行されたものであり、また、指示内容の改ざんが行われていないことを保証するための情報を攻撃遮断機器１００～攻撃遮断機器２００に対して送信する。

【００２１】攻撃遮断機器１００～攻撃遮断機器２００は、ルータなどの情報処理装置である。攻撃遮断機器１００～攻撃遮断機器２００上では、通信制御機器３からの指示と証明書発行機器４からの通信を受け取るためのアプリケーションソフトウェアおよび指示された内容に従って任意のホストからの通信を遮断するためのアプリケーションソフトウェアが動作している。

【００２２】踏み台ホスト３００～踏み台ホスト４００は、ワークステーション・サーバ・パーソナルコンピュータなどの情報処理装置である。踏み台ホスト３００～踏み台ホスト４００は、ＤＤｏＳ攻撃の実行者には本来利用できない機器であるが、ＤＤｏＳ攻撃の実行者によってインストールされたＤＤｏＳ攻撃用ソフトウェアによってＤＤｏＳ攻撃の実行者から操作可能となっている。

【００２３】攻撃実行ホスト１０は、ワークステーション・サーバ・パーソナルコンピュータなどの情報処理装置であり、ＤＤｏＳ攻撃の実行者から常に利用しうる状態となっている。

【００２４】次に、図１に示す実施の形態の動作について説明する。

【００２５】図１において、ＤＤｏＳ攻撃の実行者は、次の２つのステップを経てＤＤｏＳ攻撃を行う。最初のステップは事前の準備であり、攻撃実行ホスト１０を用いてインターネット５０を経由して踏み台ホスト３００～踏み台ホスト４００にＤＤｏＳ攻撃用ソフトウェアをインストールする。

【００２６】次のステップでは、ＤＤｏＳ攻撃の実行者は、攻撃実行ホスト１０から踏み台ホスト３００～踏み台ホスト４００に対して攻撃実行指示を行う。踏み台ホスト３００～踏み台ホスト４００は、その指示に従って攻撃対象ホスト１に対して一斉に大量のアクセスを行い、ＤＤｏＳ攻撃を行う。

【００２７】それに対して、本発明では攻撃検出機器２・通信制御機器３・証明書発行機器４の構成により攻撃遮断機器１００～攻撃遮断機器２００に対してＤＤｏＳ攻撃への防御指示を行い、ＤＤｏＳ攻撃からの防御を行う。

【００２８】次に、図１に示す各構成機器の動作について、図１および図２を参照して説明する。図２は、各構成機器の動作を説明するフローチャートである。

【００２９】攻撃検出機器２は、ＤＤｏＳ攻撃の発生を管理者からのネットワーク状況監視によって検出する。検出の手段としては、ネットワーク使用率の変化の監

視、サーバのＣＰＵ・メモリ・ＨＤＤ利用率の変化の監視など、既存の普及したネットワーク・サーバ管理技術を用いて実現する。

【００３０】攻撃対象ホスト１に対し、踏み台ホスト３００～踏み台ホスト４００までのホストを踏み台に利用したＤＤｏＳ攻撃が発生したケースを想定して説明する。

【００３１】・ＤＤｏＳ攻撃の発生

ＤＤｏＳ攻撃の実行者によって、攻撃実行ホスト１０を用いて予めＤＤｏＳ攻撃ソフトウェアのインストールされた踏み台ホスト３００～踏み台ホスト４００に対し、一斉に攻撃対象ホスト１に対する攻撃指示が出される。

【００３２】・攻撃検出機器２

攻撃検出機器２は、防御側ネットワーク５の状況を監視する（ステップ１００）。防御側ネットワーク５の管理者が、ネットワーク負荷が急激に増加したことを発見した場合、その原因となった通信を調査し、その結果、踏み台ホスト３００～踏み台ホスト４００からのアクセスが急激に増加したためであることを検出する（ステップ１０１）。管理者は、通信制御機器３に対して踏み台ホスト３００～踏み台ホスト４００からの通信を遮断するよう、通信制御機器３に対して指示を行う（ステップ１０２）。

【００３３】・通信制御機器３

通信制御機器３は、攻撃検出機器２の指示に従い、踏み台ホスト３００～踏み台ホスト４００に対する通信遮断を行うよう攻撃遮断機器１００～攻撃遮断機器２００に対して指示を行う（ステップ１０６）。また、証明書発行機器４に対して通信遮断指示の内容保証を依頼する（ステップ１０３）。

【００３４】・証明書発行機器４

ＲＳＡ公開鍵暗号化方式など既存の認証技術を用いて通信制御ブロックからの通信内容が正当なものであり、かつ改ざんされていないことを証明し、証明結果を攻撃遮断機器１００～攻撃遮断機器２００に対して送信する（ステップ１０４）。

【００３５】・攻撃遮断機器１００～２００

踏み台ホスト３００～踏み台ホスト４００が所属する個々のネットワークのうち攻撃遮断機器を備えたネットワークにおいて、通信制御機器３からの指示内容の妥当性を確認した後（ステップ１０５）、指示に従い踏み台ホスト３００～踏み台ホスト４００からの通信を遮断する（ステップ１０７）。

【００３６】例えば、踏み台ホスト３００～踏み台ホスト４００の所属する個々のネットワークのうち８割のネットワークにおいて、攻撃遮断機器１００～攻撃遮断機器２００が本発明に対応した攻撃遮断装置を実装していた場合、攻撃対象ホスト１への影響はそれまでの２割まで低減され、攻撃対象ホスト１は、ＤＤｏＳ攻撃発生以前に比べサービスが稼働可能な許容範囲内にまで復帰することが可能となる。

【００３７】一定期間の経過後（ステップ１０８）、踏み台ホスト３００～踏み台ホスト４００に対する通信遮断を解除する（ステップ１０９）。

【００３８】本発明の特徴は、従来、ＤＤｏＳ攻撃に対する防御方法として踏み台ホスト３００～踏み台ホスト４００が攻撃用ソフトウェアをインストールされないことで対応しようとしていたことに対して、踏み台ホスト３００～踏み台ホスト４００に攻撃用ソフトウェアがインストールされた場合でも、攻撃遮断機器１００～攻撃遮断機器２００においてＤＤｏＳ攻撃の影響を無視できる範囲に低減することにある。

【００３９】本発明は、ネットワークを経由したサービス妨害に対して妨害行為を受ける側の判断と責任によって妨害行為を強制的に中断させるものである。従って、ＤＤｏＳ以外の応用としては不正アクセス全般に対して本システムを適用することが可能である。次に、応用例として本システムをポートスキャンに適用した場合について説明する。

【００４０】・攻撃検出機器２

管理者からのネットワーク監視によってポートスキャンを検出することにより、他のブロックに対してポートスキャンへの対応指示を行う。

【００４１】・通信制御機器３

攻撃検出機器２の指示に従って攻撃遮断機器１００～攻撃遮断機器２００に対し、不正アクセスの発生したホストからの通信を遮断するよう指示を行う。

【００４２】・証明書発行機器４

通信制御機器３からの通信が正当なものであることを保証し、通信制御を実施することの責任が攻撃遮断機器１００～攻撃遮断機器２００の管理者でなく防御側ネットワーク５の管理者にあることを保証する。

【００４３】・攻撃遮断機器１００～攻撃遮断機器２００

通信制御機器３からの指示に従って、不正アクセスの発生したホストからの通信経路を遮断する。

【００４４】上記応用例ではポートスキャンについて示した。この最初のきっかけとなる不正アクセスの検出を他の不正アクセス検出方式で置き換えることで、検出可能な全ての不正アクセスに対して不正アクセスの被害を被る立場からの能動的な通信遮断が可能である。

【００４５】ただし、不正アクセスとみなしたホストからの通信が本当に不正アクセスなのか、何らかの理由による正当なアクセスなのかについての判断は、不正アクセスを受けた側での判断と責任において行うものであることに留意し、必要なアクセスを遮断させることにより通信相手に対して損害を与えないよう注意する必要がある。

【００４６】

【発明の効果】以上説明したように、本発明は、従来、

攻撃対象とされた場合に対応不可能と言われていたＤＤｏＳ攻撃に対して対応する現実的な手段を提供する。基本的には、インターネットを構成するネットワーク全てが本システムに対応することが望ましいが、大規模な回線業者などインターネット上での通信の基幹部分にあたるネットワークにおいて本システムを適用することで、ＤＤｏＳ攻撃の最大の特徴である膨大な量の通信を許容できる量の通信に抑えることが可能である。

【００４７】また、本発明においては、ＤＤｏＳ攻撃に対応する場合の主体が被害を受ける当事者にあるということである。従来のＤＤｏＳ攻撃への対応方法は、インターネットを構成する全てのネットワークにおいて対応することを要求とし、その責任が最新のセキュリティ技術を用いていなかった別の企業にあったとしても、当事者からそれに対する責任を問うシステムは確立されていない。

【００４８】本発明においては、最新のＤＤｏＳ攻撃に対応し得るかどうかは不正アクセスの対象となる当事者がそれを検出し得るかどうか、という当事者の責任において行うことが可能である。

【００４９】また、本発明においては、基本的に技術の更新が不要であることである。一般に、ネットワークまたはホスト単体において不正アクセスに対応したとしても、次々と新しい不正アクセスが発生し、常にネットワークまたはホスト単体を最新のセキュリティ技術を適用する必要がある。本発明においては、当事者の責任において当該不正アクセスに対する遮断を指示することを可能としているため、継続的に本技術を利用し続けることが可能である。

【００５０】インターネットを構成するネットワーク機器全てに最新のセキュリティ技術が導入されるかどうかは、それを運営する企業判断に任されている以上、一度導入すれば更新する必要のない本発明は、不正アクセスに対する現実的な対応方法を提供することが可能である。

【図面の簡単な説明】

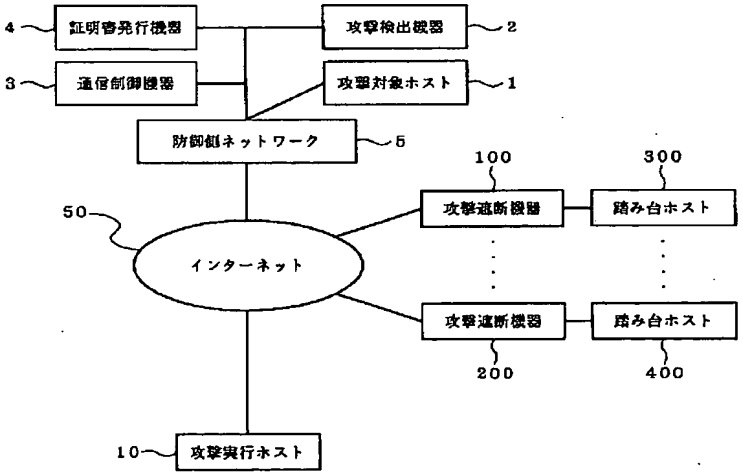
【図１】本発明の不正アクセス防御システムの実施の形態を示す構成図である。

【図２】図１に示す各構成機器の動作を説明するフローチャートである。

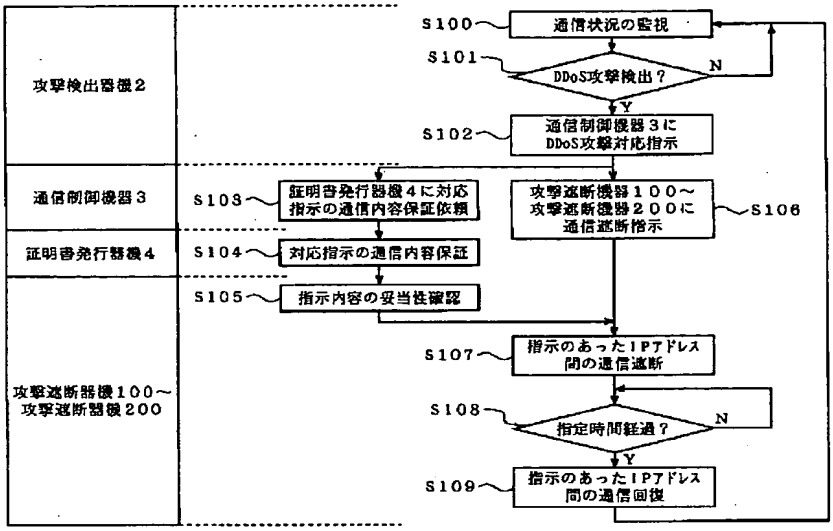
【符号の説明】

１　攻撃対象ホスト
２　攻撃検出機器
３　通信制御機器
４　証明書発行機器
５　防御側ネットワーク
１０　攻撃実行ホスト
５０　インターネット
１００～２００　攻撃遮断機
３００～４００　踏み台ホスト

【図１】



【図２】


攻撃検出器機２
通信制御機器３
証明書発行器機４
攻撃遮断器機１００～
攻撃遮断器機２００
S100
通信状況の監視
S101
DDoS攻撃検出？
N
Y
S102
通信制御機器３に
DDoS攻撃対応指示
S103
証明書発行器機４に対応
指示の通信内容保証依頼
S104
対応指示の通信内容保証
S105
指示内容の妥当性確認
攻撃遮断機器１００～
攻撃遮断機器２００に
通信遮断指示
S106
S107
指示のあったＩＰアドレス
間の通信遮断
S108
指定時間経過？
N
Y
S109
指示のあったＩＰアドレス
間の通信回復